به نام خدا

راهنمای سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه

تیرماه ۹۷

نسخه ۱,۰

پیشگفتار

در نظام ارزیابی امنیتی محصولات فتا، یکی از اسناد مورد نیاز برای انجام آزمون امنیتی، سند هدف امنیتی است. سند هدف امنیتی بر اساس اسنادی که پروفایل‌های حفاظتی نامیده می‌شوند، تهیه و تدوین می‌گردد. پروفایل‌های حفاظتی حاوی الزامات امنیتی هستند که در یک محصول افتایی می‌بایست رعایت گردد. از آنجا که متن این پروفایل‌ها پیچیده بوده و لذا تهیه سند هدف امنیتی کاری زمان‌بر برای تولیدکننده است، ساده‌سازی الزامات امنیتی موجود در پروفایل‌های حفاظتی به نحوی که برای تولیدکننده مشخص شود که چه مواردی امنیتی باید در یک محصول خاص رعایت شود، بسیار مفید خواهد بود.

سند هدف امنیتی بر اساس سند «الزامات امنیتی برنامه‌های کاربردی تحت شبکه» تدوین می‌گردد و این سند چگونگی تدوین سند هدف امنیتی را بیان می‌کند.

فهرست

۱ مقدمه

سند هدف امنیتی، یکی از اسنادی است که تولیدکننده قبل از شروع آزمون ارزیابی امنیتی، می‌بایست تدوین نماید. بر اساس استاندارد معیار مشترک (CC) این سند مبتنی بر اسنادی که پروفایل حفاظتی نام دارند، تدوین می‌گردد. متن پروفایل‌های حفاظتی اغلب ثقیل بوده به نحوی که تسلط بر مفاهیم آن‌ها زمان‌بر است. در این راستا مرکز افتا با همکاری آزمایشگاه‌های ارزیابی امنیتی و به منظور چابک‌سازی فرآیند ارزیابی امنیتی، «سند الزامات امنیتی» را جایگزین پروفایل‌های حفاظتی نموده است. هدف از سند الزامات امنیتی، ساده‌سازی مفاهیم الزامات مطرح شده در پروفایل‌های حفاظتی و کمک به تولیدکننده در جهت سرعت دادن به تدوین سند هدف امنیتی است.

این سند راهنمایی است در خصوص سند «الزامات امنیتی برنامه‌های کاربردی تحت شبکه» که به بیان مفاهیم و اصطلاحات موجود در آن و همچنین چگونگی تکمیل سند هدف امنیتی بر اساس آن می‌پردازد.

۲ اصطلاحات

مستند (Document): به هر سندی که حاوی اطلاعات برای اجرا و پشتیبانی عملیات و فعالیت‌های سازمانی استفاده می‌شوند، مستند گفته می‌شود.

رکورد (Record): مستندی که اطلاعات فعالیت‌ها، رویدادها و نتایج حاصله را نگهداری می‌کند؛ به عبارت دیگر، یک رکورد مستندی است که مدرک انجام یک فعالیت مشخص است. یک رکورد می‌تواند شامل دو یا چند مستند باشد.

رکورد ممیزی یا لاگ (Audit Record): رکوردی که حاوی اطلاعات رویدادهایی است که جهت ممیزی و بازرسی مورد نیاز است و در محل ذخیره‌سازی لاگ‌ها ذخیره می‌شود.

داده کاربر (User data): به داده‌ای گفته می‌شود که توسط کاربر ایجاد شده یا کاربر مالک آن است. فایل‌هایی که کاربر ایجاد می‌کند، محتویاتی که داخل قسمتی از برنامه یا فایلی وارد می‌کند، عکس، ویدیو، نامه و ... مثال‌هایی از داده کاربر است. همچنین این داده‌ها می‌تواند شامل مستندات تولید شده با استفاده از برنامه کاربردی مانند: Microsoft Office، نامه‌های ارجاع کار و پاسخ الکترونیکی و اسکن تصاویر باشد.

داده محصول (TSF data): داده‌ی مربوط به توابع امنیتی را می‌گویند. داده‌های پیکربندی، مجوزها و داده‌هایی که توابع تولید می‌کنند، مانند لاگ‌ها و ... نمونه‌هایی از داده‌های توابع امنیتی محصول یا داده محصول هستند.

موجودیت‌های فعال (Subjects): موجودیتی‌هایی در محصول که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهند. نقش‌هایی همچون مدیر، کاربر نهایی و ... نمونه‌هایی از موجودیت‌های فعال هستند.

همچنین این موجودیت‌ها می‌توانند فرآیندهایی باشند که از طرف کاربر مجاز عمل می‌کنند یا خود فرآیندهای داخل محصول باشند که از طرف کاربر نیز عمل نمی‌کنند.

موجودیت غیرفعال (Object): موجودیتی در محصول، که حاوی اطلاعات است و یا اطلاعات را دریافت می‌کند و توسط موجودیت‌های فعال، عملیاتی بر روی آن انجام می‌گیرد. همانند لیست کردن رکوردها توسط مدیر سیستم، حذف فایل‌ها توسط مهاجم. در مثال‌های مذکور، رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.

مشخصه‌های امنیتی(Security Attributes): یک سری مشخصه یا صفت که برای موجودیت‌های مختلف و به منظور اجرای SFR ها تعریف می‌شوند. مثلاً برای یک کاربر (موجودیت فعال): نام کاربری، کلمه عبور، مجوز دسترسی، قابلیت ممیزی، نوع اکانت و ... نمونه‌هایی از مشخصه‌های امنیتی هستند. برای یک فایل (موجودیت غیرفعال)، نوع فایل، اندازه، فرمت و ... نمونه‌هایی از مشخصه‌های امنیتی هستند.

۳ شرح محصول

محصول مورد ارزیابی، «برنامه کاربردی مبتنی بر شبکه» است که برای مدیریت رکوردها و مستندات (طبق تعاریف موجود در اصطلاحات) استفاده می‌شوند. از جمله وظایف این برنامه‌های کاربردی می‌توان به جمع-آوری، ذخیره و توزیع مستندات، پیام‌ها و فرم‌های ارتباطات اداری بین افراد اشاره نمود (شکل ۱).

به‌طور کلی برنامه کاربردی تحت شبکه برای رکوردها و مستندات الکترونیکی از فعالیت‌های زیر استفاده می‌کند:

- ثبت رکوردهای الکترونیکی
- مدیریت گردش کار رکوردهای الکترونیکی
- ایجاد و مدیریت فرآیندهای آرشیو
- انجام امور جستجو و گزارش دهی
- قابلیت مدیریت کاربران
- پشتیبانی از سازوکارهای امن‌سازی ارتباطات
- سازوکارهای احراز هویت و کنترل دسترسی

شکل ۱: مؤلفه‌های برنامه کاربردی تحت شبکه

۱,۳ مؤلفه‌های محیط عملیاتی

یک برنامه کاربردی تحت شبکه، یک برنامه اجرایی بر روی بستر شبکه است و با مؤلفه‌های شبکه در تعامل است که بر روی سیستم‌عامل اجرایی در محیط شبکه اجرا می‌گردد. محصول با واحد/واحدهای ذخیره‌سازی به منظور نگهداری رکوردها و با مؤلفه‌های ممیزی به منظور نگهداری رکوردهای ممیزی در تعامل است؛ در ادامه، این مؤلفه‌ها با جزئیات شرح داده می‌شوند.

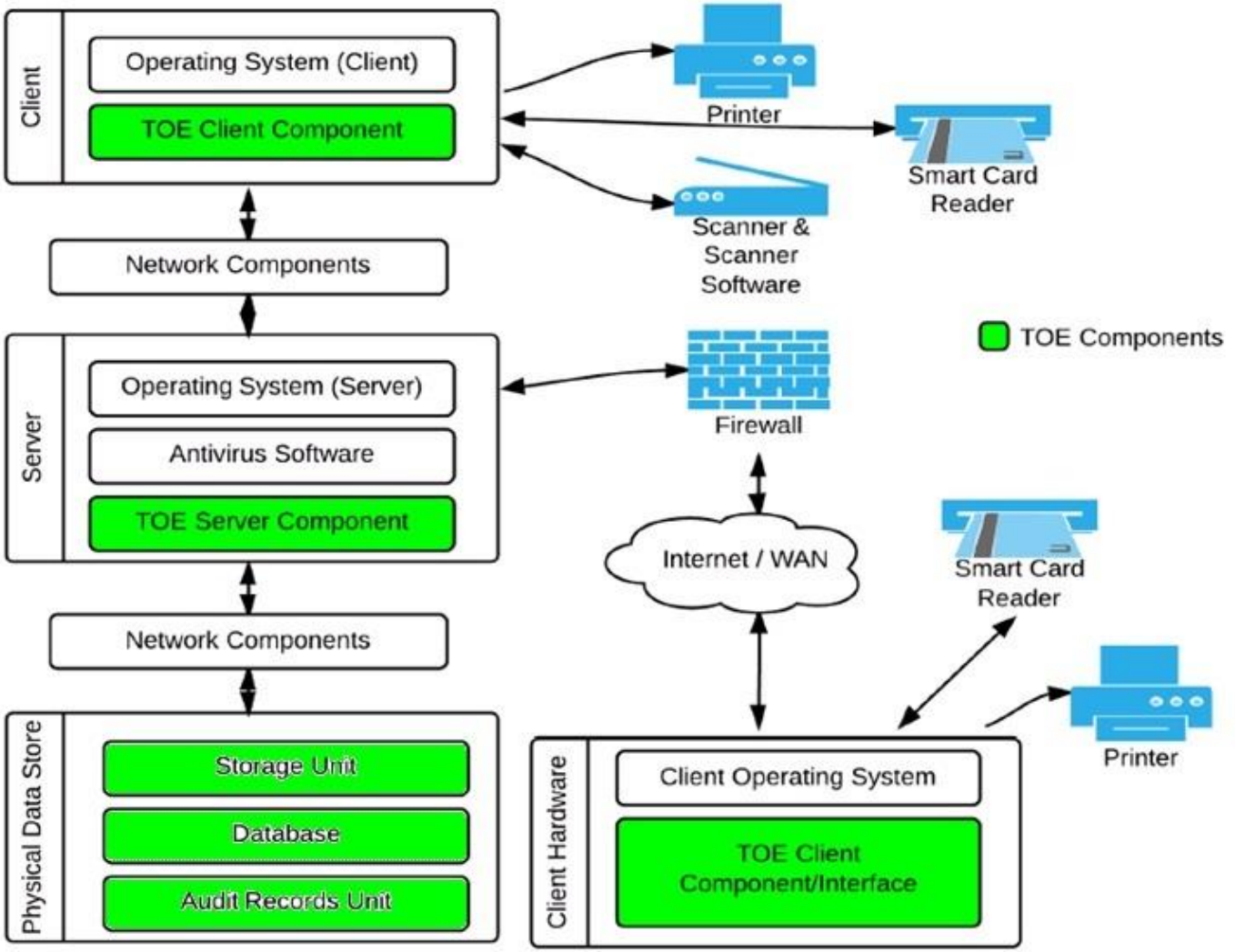
محیط عملیاتی محصول شامل مؤلفه‌های نرم‌افزاری و سخت‌افزاری و همچنین ویژگی‌های کارکردی و امنیتی اصلی است که در این سند پوشش داده شده‌اند. شکل ۲ بیانگر سخت‌افزار و نرم‌افزارهایی است که محصول با آن‌ها در تعامل است. این شکل چگونگی تعاملات محصول با محیط عملیاتی را نمایش می‌دهد:

سرور: سرور مؤلفه سخت‌افزاری است که مؤلفه سروری محصول بر روی آن اجرا می‌گردد. سرور می‌تواند به صورت فیزیکی یا مجازی باشد، پیکربندی و قابلیت‌های سرور می‌تواند با توجه به تعداد کاربران، تعداد اتصالات و غیره متفاوت باشد.

سیستم کاربر: سخت‌افزار و سیستم‌عاملی است که به کاربران اجازه دسترسی به محصول را می‌دهد. این مؤلفه معمولاً یک کامپیوتر بوده ولی می‌تواند یک تبلت یا گوشی هوشمند نیز باشد، در این پروفایل حفاظتی فرض شده که کلاینت یک کامپیوتر است. دو نوع کلاینت وجود دارد. یکی برای کاربر پایانی و نوع دیگر برای کاربرانی که رکوردها و مستندات را به داخل محصول وارد می‌نمایند. اتصالات بین کلاینت‌ها و مؤلفه‌های مرکزی محصول می‌تواند به صورت اینترنت، اینترانت یا VPN باشد.

سیستم‌عامل: محصول بر روی یک سیستم‌عامل اجرا می‌شود و ارتباطات بین محصول و واحد ذخیره-سازی، واحد رکوردهای ممیزی، مؤلفه‌های شبکه و سرور توسط سیستم‌عامل مهیا می‌شود.

مؤلفه‌های شبکه: محصول به واسطه سیستم‌عامل و سرور با مؤلفه‌های شبکه در تعامل است. لازم است اتصالات شبکه بین کلاینت‌ها و سرور محصول به صورت امن باشد. کلاینت محصول قادر به انجام اقداماتی همانند چاپ، اسکن و غیره است. اتصالات بین این مؤلفه‌ها و سرور معمولاً به صورت یک شبکه محلی است.



شکل ۲: محیط عملیاتی محصول

فایروال: دسترسی اینترانت به‌وسیله‌ی این مؤلفه، امن می‌شود.

نرم‌افزار آنتی‌ویروس: نرم‌افزار آنتی‌ویروس جهت بررسی مستندات و رکوردهای ورودی استفاده می‌شود.

پایگاه داده: محصول با یک پایگاه داده برای حفظ و نگهداری داده‌های خود در تعامل نزدیک است. رکوردها و مستندات می‌توانند در پایگاه داده و یا به صورت مجزا حفظ و نگهداری شوند. در زمان نیاز به یک مجموعه داده خاص، یک درخواست به پایگاه داده ارسال و نتایج آن گرفته می‌شود.

واحد ذخیره‌سازی مستندات و رکوردها: رکوردها و مستندات می‌توانند به صورت مجزا در سمت سروری که محصول بر روی آن اجرا می‌گردد باقی مانده تا محصول به آسانی تحت تأثیر آسیب‌پذیری امنیتی بالقوه در واحد ذخیره‌سازی قرار نگیرد.

واحد ذخیره رکوردهای ممیزی: همانند واحدهای ذخیره‌سازی، واحد رکوردهای ممیزی در سمت سروری قرار می‌گیرد که محصول بر روی آن اجرا می‌گردد. این واحد می‌تواند به صورت مؤلفه مجزا و یا بخشی از واحد ذخیره‌سازی باشد.

کارت‌خوان هوشمند: کارت‌خوان یک مؤلفه سخت‌افزاری است که دارای گواهی مورد اعتماد است و برای امضاء اسناد الکترونیکی استفاده می‌شود. در حال حاضر رایج‌ترین نوع کارت‌خوان توکن USB است. از آنجائی که این مؤلفه مبتنی بر سخت‌افزار بوده و به شبکه متصل نیست، سطح بالایی از امنیت را فراهم می‌نماید؛ بنابراین می‌تواند برای احراز هویت استفاده شود.

اسکنر و درایور آن: کاربرانی که برای اسکن نمودن مجاز هستند، رکوردها و مستنداتی که به شکل کاغذی دریافت می‌کنند را اسکن می‌نماید.

پرینتر: مؤلفه‌ای است که به کاربران محصول مطابق با مجوز کاربر، اجازه چاپ هر رکورد یا مستندی را می‌دهد.

۲,۳ انواع کاربران

حداقل دو دسته کاربر برای محصول وجود دارد:

- کاربر عادی
- مدیر سیستم

علاوه بر نقش‌های لیست شده در بالا، محصول ممکن است دارای نقش‌های دیگری نیز باشد. در صورت وجود نقش‌های دیگر لازم است در سند هدف امنیتی ذکر گردد.

کاربر عادی: کاربر عادی از محصول به صورت یک جعبه سیاه استفاده می‌کند و قادر به مدیریت داده تحت مالکیتش نیز است. کاربر عادی در صورت داشتن مجوز می‌تواند رکوردها و مستندات را جستجو، لیست و مشاهده نماید. علاوه بر آن کاربر عادی می‌تواند سند یا رکورد جدیدی ایجاد نماید یا سند و رکوردی که مالک آن است را حذف نماید. این نوع کاربر می‌تواند مستندات را بایگانی نماید و باید به اسناد بایگانی شده خود دسترسی داشته باشد.

مدیر سیستم: مدیر، دارای مجوز خاص برای مدیریت محصول است. مدیر سیستم می‌تواند یک نفر باشد یا برای بخش‌های مختلف محصول، مدیران مختلفی وجود داشته باشد، همانند مدیر پایگاه داده، مدیر شبکه، مدیر برنامه کاربردی و غیره. همچنین مدیر دارای سطح دسترسی کامل برای دسترسی به برنامه کاربردی، پایگاه داده، فایل سیستم و دیگر موجودیت‌ها است.

۳,۳ ویژگی‌های امنیتی محصول

احراز هویت و مجوزدهی: عملیات احراز هویت و مجوزدهی باید به طور مؤثری انجام شود. احراز هویت به طور کلی با بررسی و تائید نام کاربری و کلمه عبور صورت می‌گیرد. لازم به ذکر است برای مدیریت کلمات عبور مورد استفاده باید روال‌های امن وجود داشته باشد. در صورتی که محصول به سطح بالایی از امنیت نیاز داشته باشد، از یک سازوکار احراز هویت دیگر یا ترکیبی از دو و یا بیشتر از دو سازوکار استفاده می‌شود. از جمله سازوکارهای احراز هویت می‌توان به وارسی نام کاربری و کلمه عبور، وارسی SMS، احراز هویت از طریق یک برنامه موبایل، گواهی دیجیتال، وارسی بیومتریک و توکن سخت‌افزاری اشاره نمود.

کنترل دسترسی: محصول، قابلیت‌های لازم برای محدود کردن دسترسی را دارد، به طوری که تنها موجودیت‌های مجاز، به داده و کارکردهای محصول دسترسی دارند. برای کاربران مجاز، کنترل دسترسی معمولاً با استفاده از داده احراز هویت انجام می‌گیرد. محصول ممکن است همچنین آدرس‌های IP اتصالات فعال را کنترل نماید و تنها به آدرس‌های IP از پیش تعریف شده در یک بازه زمانی خاص برای عملیات حساس اجازه اتصال دهد.

ممیزی: محصول رکوردهای ممیزی را به صورت خودکار به منظور ردیابی و کنترل فعالیت‌های کاربر بر روی دارایی‌ها، تغییرات کنترل دسترسی و پیکربندی جمع‌آوری می‌نماید. محتوای رکوردهای ممیزی، روش‌های حفظ رکورد و فواصل نگهداری را می‌توان توسط رابط گرافیکی محصول پیکربندی نمود. هیچ فردی جز افرادی همچون مدیر که محصول، آن‌ها را مجاز نموده، امکان تغییر یا حذف محتویات رکوردهای ممیزی را ندارند.

مدیریت: محصول، برای مدیریت کاربران و دسترسی‌ها واسط‌های مدیریتی لازم را فراهم می‌نماید. سرعت و دقت این واسط‌ها در تصمیم‌گیری در طول یک رخداد امنیتی بسیار مهم است.

صحت رکوردها و بررسی منابع: حذف یا تغییر هر رکورد توسط محصول مجاز نیست؛ بنابراین، دسترسی و تغییر سند و/یا فراداده[۱] آن باید محدود گردد. صحت رکوردهای ذخیره شده، توسط روشی مانند امضای دیجیتال مهیا می‌گردد.

پشتیبان‌گیری: عملیات پشتیبان‌گیری بر روی داده، مستندات و رکوردهای ممیزی که محصول از آن‌ها محافظت می‌کند، می‌تواند توسط خود محصول و یا یک ابزار خارجی که بدین منظور استفاده می‌شود، صورت گیرد. عملیات پشتیبان‌گیری نسبت به عدم از دست رفتن داده اطمینان می‌دهد.

کنترل گردش مستندات و اطلاعات: حداکثر اندازه فایل می‌تواند به صورت پویا برای هر نوع سند تعریف شود. محصول، فضای خالی ذخیره‌سازی را در نظر گرفته و در برابر سرریز ذخیره‌سازی اقدامات احتیاطی لازم را اتخاذ می‌کند. علاوه بر این تنها کاربران مجاز، دارای مجوز صدور و ارسال هر رکورد و یا سندی هستند.

[۱] Metadata

درهم‌سازی/رمز کردن داده حساس: مثالی از داده حساس، کلمات عبور یا رکوردهای محرمانه است. داده حساس بر روی محصول به صورت واضح ذخیره نمی‌شوند و با سازوکاری از آن‌ها محافظت می‌شود. همچنین باید رکوردهای محرمانه به صورت رمز شده نگهداری شوند. ارتباط بین کاربر و سرور باید با استفاده از رمزنگاری امن شود تا از افشای محتوی رکوردها جلوگیری گردد. روش درهم‌سازی و رمزنگاری انتخاب شده باید به اندازه کافی قوی باشد به طوری‌که توسط فناوری‌های امروزی در یک بازه‌ی منطقی قابل شکسته شدن نباشد.

۴,۳ راهنمای تدوین سند هدف امنیتی

در سند «الزامات امنیتی برنامه‌های کاربردی تحت شبکه»، مجموعه الزامات در قالب دسته‌های (که مبتنی بر کلاس‌ها در پروفایل حفاظتی مربوطه هستند) مختلفی مطرح شده‌اند که تولیدکننده محصول باید با بررسی محصول خود، موارد خواسته شده را تکمیل نماید. برای تکمیل هر یک از موارد مطرح شده، دو ستون وجود دارد. ستون اول در صورتی علامت زده می‌شود که الزام بیان شده در محصول پیاده‌سازی شده است و در ستون دوم توضیحاتی در مورد چگونگی پیاده‌سازی آن بیان می‌شود.

برخی از الزامات مطرح شده در این سند، دارای زیر بخشی است که شامل تعدادی الزام است. این بدان معنی است که الزام سطح اول (الزام اصلی) در صورتی برآورده می‌شود که تمامی الزامات مطرح شده در بخش زیرین (الزامات تکمیلی) در محصول موجود باشد مگر آنکه در آن بخش بیان شده باشد که «**وجود یک مورد لازم و کافی است**»، در آن صورت پیاده‌سازی یکی از موارد موجود در بخش زیرین، الزام اصلی را برآورده می‌سازد.

لازم به توضیح است که الزامات موجود در سند، همان مواردی است که در آزمون ارزیابی امنیتی بررسی می‌شود و در صورتی که هر یک از آن‌ها در محصول پیاده سازی نشده باشد، به‌عنوان عدم انطباق تلقی شده و می‌بایست توسط تولیدکننده رفع گردد.

۵,۳ نمونه‌ای از الزامات تکمیل شده

برای توضیح بیشتر در خصوص چگونگی تدوین سند هدف امنیتی بر اساس سند «الزامات امنیتی برنامه کاربردی تحت شبکه»، الزامات مربوط به دسته (کلاس) پشتیبانی از رمزنگاری، در جدول (۱) تکمیل شده است. در مواردی که یک الزام در محصول پیاده‌سازی نشده است (پشتیبانی نمی‌شود)، در قسمت توضیحات، علت بیان گردد.

جدول (۱) نمونه‌ای از الزامات امنیتی تکمیل شده

شماره الزام	کلاس رمزنگاری				توضیحات
۱	**محصول باید قابلیت رمزنگاری یا ماژول رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده ISO 18033-3) با توجه به موارد زیر انجام دهد.**			☑	محصول از مد عملیاتی GCM با طول کلید ۲۵۶ بیتی استفاده می‌کند.
	مد عملیاتی که الگوریتم از آن استفاده می‌کند را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)	مد عملیاتی CBC و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در NIST SP 800- 38A)	☐		
		مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در NIST SP 800- 38D)	☑		
		مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در ISO10116)	☐		
۲	**محصول باید بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب**			☑	در محصول از الگوریتم SHA-1 با اندازه خلاصه پیام

	می‌نماید؛ توانایی تولید داده درهم‌سازی‌شده (هش) را داشته باشد، بنابراین باید برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده نماید.				۲۵۶ بیتی استفاده می‌شود.
	الگوریتم و اندازه خلاصه پیام مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)	الگوریتم SHA-1 با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲ بیتی	☑		
		الگوریتم SHA-256 با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲ بیتی	☐		
		الگوریتم SHA-384 با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲ بیتی	☐		
		الگوریتم SHA-512 با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲ بیتی	☐		
۳	**در صورتی که محصول از الگوریتم‌های رمزنگاری نامتقارن استفاده می‌نماید، لازم است که تولید کلید رمزنگاری را بر اساس موارد زیر انجام دهد.**			☑	در محصول از ECC با منحنی‌های NIST به همراه P-256 استفاده می‌شود.
	الگو و طول کلید یا نوع منحنی مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی	الگوهای RSA با کلیدهای رمزنگاری ۲۰۴۸ بیت یا بزرگ‌تر (بر اساس FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.3)	☐		
		الگوهای ECC با استفاده از منحنی‌های NIST و P-256 یا P-384 یا P-521 (بر اساس FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.4)	☑		

	است.)	الگوهای FFC با کلیدهای رمزنگاری ۲۰۴۸ بیت یا بزرگ‌تر (بر اساس FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS)، پیوست B.1)	☐		
۴	**در صورتی که در محصول تولید کلید رمزنگاری وجود دارد، نیاز است که تخریب کلید رمزنگاری نیز بر اساس موارد زیر، صورت پذیرد. (اختیاری)**		☑		نابودی کلید از طریق بازنویسی ساده به کمک مقدار تصادفی صورت می‌گیرد.
	روش نابودی کلید مشخص گردد. (وجود یک مورد لازم و کافی است)	نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یک‌ها، مقدار تصادفی، مقدار جدیدی از کلید)	☑		
		نابودی با استفاده از یک واسط مشخص	☐		
		از طریق توابع امنیتی محصول	☐		
		سایر موارد	☐		
۵	**در صورتی که در محصول از امضاء دیجیتال پشتیبانی می‌شود، نیاز است که سرویس‌های امضای رمزنگاری (تولید و تأیید) بر اساس الگوریتم‌های رمزنگاری زیر انجام گیرد. (اختیاری)**		☒		محصول از امضاء دیجیتال پشتیبانی نمی‌کند. علت: ...
	الگوریتم و اندازه کلیدهای مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی	الگوریتم‌های امضاء دیجیتال RSA با کلیدهای رمزنگاری ۲۰۴۸ بیت یا بزرگ‌تر (بر اساس FIPS PUB 186-4، استاندارد امضاء دیجیتال (DSS) بخش ۵،۵، الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA-PKCS1v1_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال ۲ یا الگوی امضای دیجیتال ۳)	☐		

	است.)	الگوریتم‌های امضاء دیجیتال ECDSA با کلیدهای رمزنگاری ۲۵۶ بیت یا بزرگ‌تر (بر اساس ISO/IEC 14888-3 بخش ۶,۴، استاندارد امضای دیجیتال (DSS) بخش ۶ و پیوست D، با استفاده از منحنی‌های P-256 یا P-384 یا P-521)	☐		